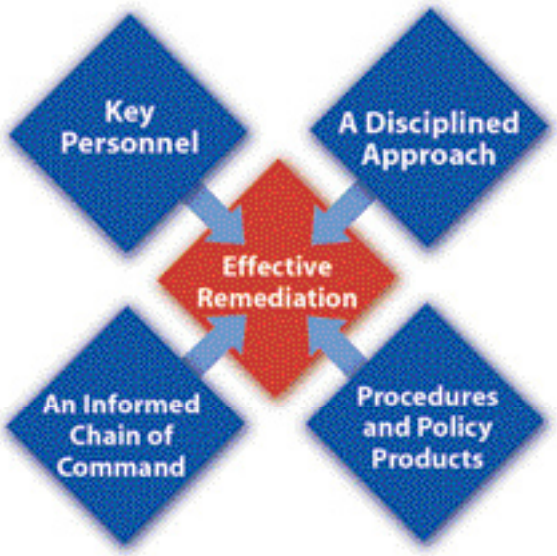


Figure 3 illustrates the four factors that are critical to successful remediation within a disciplined approach.

to successful remediation, as shown in Figure 3: (1) procedures/policy; (2) an informed chain of command; (3) key personnel; and (4) a disciplined approach. The first three factors are controlled by the command.

The ***Remediation: ASAP*** training course provides the disciplined approach necessary to develop and implement a successful remediation plan.

The effectiveness of the approach taught within the course depends on the involvement of key installation and tenant command personnel, the support of an informed chain of command and a thorough understanding of the particular policies and procedures applicable to the installation.

The goal of successful remediation is to reduce vulnerabilities while achieving maximum return on investment and focusing limited resources on the most essential assets.

Remediation can provide proactive protection against criminal and natural acts that threaten to disrupt mission accomplishment. Because proper remediation may actually thwart or minimize the chances of a terrorist attack, it makes sense to "harden" those assets believed critical to the warfighter's mission through remediation actions.

The DON CIP Program's Command Remediation Visit initiative is a valuable tool that supports mission assurance by promoting effective remediation strategies and plans.

To access CIP policy and guidance, go to the DON CIO Web site at http://www.doncio.navy.mil, click on the Project Teams tab, then click on Critical Infrastructure Protection.

CHIPS

Coalition Interoperability Reaches New Heights in RIMPAC 2006

Forty ships, six submarines, 160 aircraft and more than 19,000 personnel from Australia, Canada, Chile, Japan, Peru, South Korea, the United Kingdom and the United States engaged in seamless communications during RIMPAC 2006 …

By Lt. Cmdr. Vince Augelli, Lt. Cmdr. Dave Samara and Lt. Cmdr. George Haw

Commander, U.S. Third Fleet achieved unprecedented coalition interoperability during the latest Rim of the Pacific (RIMPAC) exercise. Scheduled by the Commander, U.S. Pacific Fleet, RIMPAC is a biannual multinational exercise conducted in the Hawaiian operating area. The exercise, conducted from June 26 through July 28, featured 40 ships, 6 submarines, 160 aircraft and more than 19,000 personnel from Australia, Canada, Chile, Japan, Peru, South Korea, the United Kingdom and the United States.

Cooperative Maritime Forces Pacific

The major advance in RIMPAC '06 was the introduction of the Combined Enterprise Regional Information Exchange System (CENTRIXS) community of interest called the Cooperative Maritime Forces Pacific (CMFP).

CMFP offered Web-browsing, e-mail, chat and the common operational picture over a secure network. While different security enclaves within CENTRIXS have been used in previous RIMPAC exercises, this was the first time that all participants had access to a common network.

A comparison between RIMPAC '04 and RIMPAC '06 will better illustrate this. The January-March 2005 edition of CHIPS featured an article *(available at http://www.chips.navy.mil/archives/05_Jan/web_pages/RIMPAC.htm)* describing the C4I architecture for RIMPAC 04. It included four different security enclaves for coalition releasability: CENTRIXS FOUR EYES – used by U.S., U.K., Canadian and Australian forces; CENTRIXS-J – used by U.S. and Japanese forces; CENTRIXS-R – used by U.S., South Korean and Chilean forces; and SIPRNET – used by U.S. forces.

For these four different security enclaves partial interoperability was achieved through the use of air-gapping, replication and a high assurance mail guard.

Of note, only the exercise's Task Force Commander/Combined Forces Maritime Component Commander (CFMCC) ashore in Pearl Harbor enjoyed access to all four enclaves. All other participants were dependent on the redistribution of information from this central node. While cleverly done, time delays were unavoidable.

In contrast, CENTRIXS Cooperative Maritime Forces Pacific was accessible to CFMCC headquarters, the outlying shore sites including all component commanders and commanders of maritime task forces, and every U.S. and coalition ship in the entire exercise. Information that was seen at Pearl Harbor was available afloat at the same time. This led to an unprecedented level of operational execution and planning.

CMFP Provides Unprecedented Interoperability

CMFP is a new community of interest in the existing CENTRIXS Global Counterterrorism Task Force (GCTF) security enclave. It was developed by Mr. Bob Stephenson, chief technology officer for command, control, communications, computers and intelligence operations at the Space and Naval Warfare Systems Command, and Mr. Tim Gannon, a division head from the Naval Network Warfare Command. The CMFP was used on a large scale for the first time during RIMPAC '06.

"We were a victim of our own success. Everyone wanted more CMFP."

– admiral participating in RIMPAC 2006

Based at the Pacific Regional Network Operations Center at Wahiawa, Hawaii, CMFP was the core of the integrated planning and execution in RIMPAC '06. Servers were also located at Esquimalt, British Columbia, and the Australian NOC at Canberra, as shown in Figure 1.

Ships connected to CMFP through satellite connection. U.S. ships had Internet Protocol connectivity through the Defense Satellite Communications System super high frequency X-band termination or dedicated International Maritime Satellite Bravo (Inmarsat-B) lease.

Coalition ships used dedicated Inmarsat-B leases with the exception of HMAS Manoora, which used a commercial Ka-band termination to Australia. Notably, this was the first RIMPAC in which each ship had continuous round-the-clock CENTRIXS connectivity versus intermittent dial-up connection.

The RIMPAC Combined Air Operations Center was established for the first time at Kenney Headquarters at Hickam Air Force Base. The RIMPAC Combined Forces Air Component Commander was able to leverage Kenney's tremendous capabilities and infrastructure while enjoying the same CMFP connectivity with coalition forces.

The core of the Combined Forces Air Component Commander's planning was conducted on a special version of the Theater Battle Management and Core System that was created for coalition use.

The result was a reliable, secure network which succeeded in attracting an unprecedented number of collaborators.

Whereas CENTRIXS access in previous exercises had been largely limited to watchstations, CMFP attracted hands-on attention from numerous participants throughout the chain of command up to flag level.

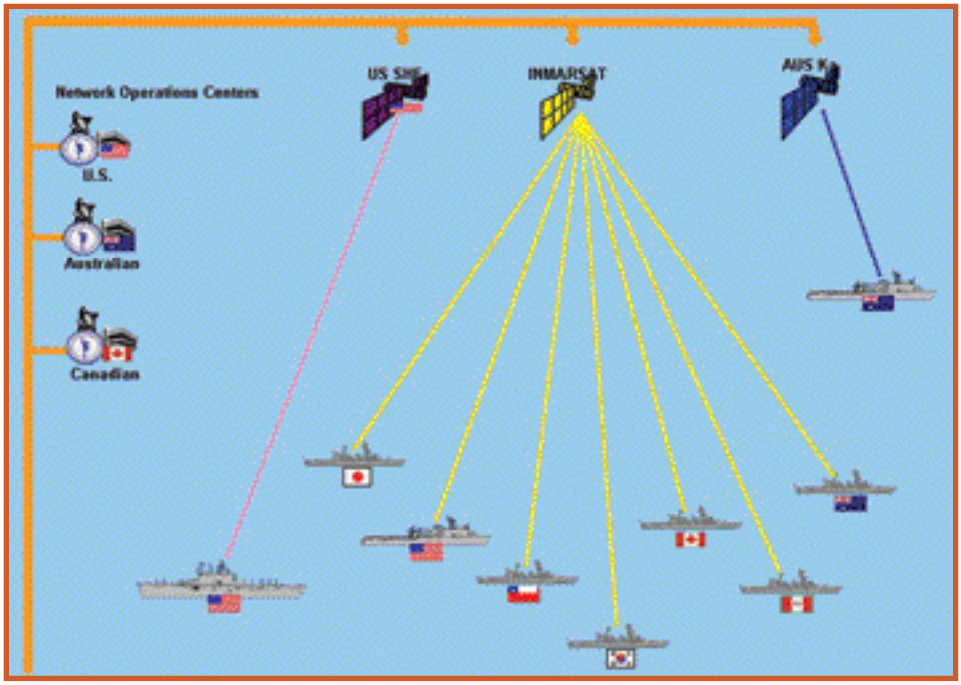
One admiral aptly summed up the phenomenon by noting that, "We were a victim of our own success. Everyone wanted more CMFP."

Hopefully, that will indeed be the case in RIMPAC 2008.

The authors were members of the Third Fleet staff for RIMPAC '06. Lt. Cmdr. Augelli is the fleet communications officer, Lt. Cmdr. Samara is the knowledge manager and Lt. Cmdr. Haw is the fleet information systems officer.

CHIPS

Figure 1. RIMPAC 2006 CENTRIXS CMFP Architecture.



CHIPS 25th Anniversary

CHIPS celebrates 25 years in publication in 2007 as the Department of the Navy Information Technology Magazine.

Our founding motto — Dedicated to Sharing Information, Technology and Experience, aligns with our goal — to deliver knowledge superiority to the warfighter.

CHIPS is sponsored by the DON IT Umbrella Program of contracts and the Department of the Navy Chief Information Officer (DON CIO). Each issue contains a message from the DON CIO and articles highlighting the latest IT policies and initiatives in the DON and Department of Defense.

The Umbrella Program team assembles the latest information regarding the Umbrella Program contracts and Blanket Purchase Agreements (BPAs). Each issue contains an easy to use shopping guide — Under the Contract — spotlighting better than GSA pricing for all your technology needs.

Every issue is packed with cutting-edge technology topics, such as FORCEnet; knowledge dominance; C4ISR and network-centric warfare programs; e-business; e-learning; professional development — and interviews with top leadership from the DON and DoD.

We welcome articles from our readers! Please help us celebrate by submitting your articles and ideas to the CHIPS editors at chips@navy.mil.

CHIPS is published quarterly. Articles must be approved by your public affairs office and your chain of command prior to submitting your article to CHIPS.

CHIPS writing guidelines are available on our Web site at http://www.chips.navy.mil/chipsguidelines.html. For assistance, and to request a subscription or extra copies of CHIPS, contact a CHIPS editor at (757) 444-8704 or DSN 564.

Thank you for your support! It has been a pleasure for us to serve you, and we look forward to serving you for another 25 years! CHIPS